

Требования по обеспечению информационной безопасности

Применяется в случае модернизации, реконструкции или создания СПД, АСУ ТП, ТМ, СДТУ, РЗА, АСМД и дистанционного управления КА.

Порядок создания подсистемы информационной безопасности, построение этапов работ, а также разработка технической и рабочей документации должны соответствовать ГОСТ Р 51583-2014 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения».

Обеспечить создание подсистемы информационной безопасности, а также обеспечить выполнение:

- требований 187-ФЗ от 26.07.2017г. «О безопасности критической информационной инфраструктуры Российской Федерации» и подзаконных актов;
- требований Приказа ФСТЭК от 14 марта 2014 г. № 31 - не ниже 3 класса защищенности автоматизированной системы управления;
- требований РД «Автоматизированные системы. Защита от несанкционированного доступа. Классификация автоматизированных систем и требования по защите информации» не ниже уровня 1 Г;
- требований Положения ПАО «Россети» «О единой технической политике в электросетевом комплексе»;
- средства защиты информации должны соответствовать требованиям не ниже 6-го или более высокого уровня доверия («Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий», утвержденные приказом ФСТЭК России от 02.06.2020 N 76);

Обеспечить нейтрализацию всех угроз информационной безопасности, актуальных для объектов защиты.

В случае модернизации, реконструкции или создания автоматизированной системы мониторинга и диагностики энергетического оборудования, обеспечить выполнение требований Приказа Министерства энергетики РФ от 06.11.2018 №1015 «Об утверждении требований в отношении базовых (обязательных) функций и информационной безопасности объектов электроэнергетики при создании и последующей эксплуатации на территории Российской Федерации систем удаленного мониторинга и диагностики энергетического оборудования».

В случае организации дистанционного управления оборудованием:

- обеспечить выполнение требований Приказа Минэнерго России от 26.12.2023 № 1215 "Об утверждении дополнительных требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры, функционирующих в сфере электроэнергетики, при организации и осуществлении дистанционного управления технологическими режимами работы и эксплуатационным состоянием объектов электроэнергетики из диспетчерских центров субъекта оперативно-диспетчерского управления в электроэнергетике";
- необходимо руководствоваться требованиями ГОСТ Р 71077-2023 Единая энергетическая система и изолированно работающие энергосистемы. Оперативно-диспетчерское управление. Дистанционное управление. Правила применения защищенных протоколов при организации информационного обмена.

Применяемое оборудование должно быть включено в Реестр промышленной продукции, произведенной на территории Российской Федерации.

Применяемое программное обеспечение должно быть включено в Единый реестр российских программ для электронно-вычислительных машин и баз данных.

Применяемые средства защиты информации, а также операционные системы, применяемые для функционирования средств защиты информации, должны быть сертифицированы ФСТЭК России.

Применяемые программные и программно-аппаратные средства СПД, АСУ ТП, ТМ, СДТУ, РЗА, АСМД и дистанционного управления КА должны быть допущены к применению на объектах ПАО "Россети", в соответствии с требованиями Приказа ПАО «Россети» от 26.07.2023 № 305 «Об утверждении документов в области проверки качества (аттестации) оборудования, материалов и систем», а также соответствовать требованиям безопасности информации в группе компаний «Россети», согласно Положению, утвержденному Приказом ПАО «Россети» от 24.12.2025 № 682 «Об утверждении Положения об оценке соответствия программных и программно-аппаратных средств требованиям безопасности информации в группе компаний «Россети»» (включены в реестр объектов, прошедших оценку соответствия требованиям по информационной безопасности).

Операционные системы, применяемые в программных и программно-аппаратных средствах СПД, АСУ ТП, ТМ, СДТУ, РЗА, АСМД и дистанционного управления КА должны быть сертифицированы ФСТЭК России и/или пройти оценку соответствия требованиям по безопасности информации в составе средств сети передачи данных, АСУТП, телемеханики, согласно Положению, утвержденному Приказом ПАО «Россети» от 24.12.2025 № 682 «Об утверждении Положения об оценке соответствия программных и программно-аппаратных средств требованиям безопасности информации в группе компаний «Россети»».

Операционные системы, не имеющие действующего сертификата соответствия ФСТЭК России и/или не прошедшие оценку соответствия требованиям по безопасности информации ПАО «Россети» (в составе СПД, АСУ ТП, ТМ, СДТУ, РЗА, АСМД и дистанционного управления КА), к применению, в составе данных средств, не допускаются. Данное требование распространяется на все уровни архитектуры систем. Копии действующих сертификатов и/или выписки из реестра должны быть представлены в составе проектной и рабочей документации.

При проектировании и выполнении работ, учесть мероприятия, выполняемые в рамках смежных проектов.

Тома проектной и рабочей документации в части информационной безопасности и тома в части защищаемых объектов информационной инфраструктуры (СПД, АСУ ТП, ТМ, СДТУ, РЗА, АСМД, дистанционного управления КА) согласовать со структурным подразделением информационной безопасности филиала, Департаментом информационной безопасности ИА Общества и филиалом АО «СО ЕЭС» - «Московское РДУ». (в случае организации обмена информацией с филиалом АО «СО ЕЭС» - «Московское РДУ»).

Участник торгово-закупочных процедур или член коллективного участника, чьими силами планируется выполнение работ в части обеспечения информационной безопасности, на момент подачи заявки и выполнения работ должен отвечать следующим требованиям по наличию:

- Лицензии ФСТЭК на деятельность по технической защите конфиденциальной информации согласно п.п. б), е) ст.4 Положения введенного Постановлением Правительства РФ от 03.02.2012 года № 79;

– Лицензии ФСБ на осуществлении работ по пунктам 12-14, 21-23 «Перечня выполняемых работ и оказываемых услуг, составляющих лицензируемую деятельность, в отношении шифровальных (криптографических) средств», утвержденного Постановлением Правительства РФ 16.04.2012 года № 313.

Заместитель директора департамента –
начальник управления информационной безопасности



В.А. Андрианов